13 July 2015

NORTH DAKOTA

HOMELAND SECURITY

Cyber Summary

The North Dakota Open Source Cyber Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Cyber Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Table of Contents

North Dakota

Nothing Significant to Report

Regional

Nothing Significant to Report

National

(National) **IRS can't update woefully out-of-date Windows server because it can't find some of them.** The Treasury Inspector General for Tax Administration at the U.S. Department of the Treasury released a report which found that the Internal Revenue Service was unable to locate 1,300 workstations during its attempt to update its Microsoft software from Windows XP to Windows 7. The report also determined that the bureau had several thousand servers still running Windows Server 2003 and lacked proper oversight, among other security risks. http://www.nextgov.com/cio-briefing/2015/10/irs-cant-update-woefully-out-date-windows-servers-because-it-cant-find-some-them/122770/

International

(International) **America's thrift store hit by cyber attack, Birmingham-based company says credit card data exposed.** Birmingham-based America's Thrift Store reported October 12 that cyber criminals from Eastern Europe accessed its systems through a third-party provider and installed malwares onto its system, allowing unauthorized access to customers' payment card numbers from September 1 – September 27. Officials reported the malware has since been removed and the U.S. Secret Service is investigating the breach. http://www.al.com/news/index.ssf/2015/10/americas_thrift_store_hit_by_c.html

(International) Authorities seize servers to disrupt Dridex botnet. U.S. and European authorities worked with private cybersecurity organizations to disrupt the activities of the Dridex information-stealing botnet by poisoning the peer-to-peer (P2P) network of each sub-botnet, redirecting infected systems' communications from the botnet to a sinkhole. The botnet resulted in estimated losses of $10 million in the U.S., and authorities are seeking to extradite one of its administrators who was arrested in Cyprus in August. http://www.securityweek.com/authorities-seize-servers-disrupt-dridex-botnet

(International) Adobe Flash Player zero-days used by hackers linked to Russian government. Security researchers from Trend Micro warned that attackers in the Operation Pawn Storm cyber-espionage campaign are exploiting unpatched zero-day vulnerabilities in Adobe Flash Player in an effort to trick members of overseas government departments and ministries to access Web sites hosting malicious code. The group previously targeted high-profile government targets worldwide, as well as the North Atlantic Treaty Organization (NATO) and the U.S. White House. http://news.softpedia.com/news/adobe-flash-player-zero-days-used-by-hackers-linked-to-russian-government-494509.shtml

(International) Attackers can use Siri, Google Now to secretly take over smartphones. Security researchers from the French Network and Information Security Agency discovered that attackers could use a laptop running GNU Radio, an amplifier, a universal software radio peripheral (USRP) software-defined radio, and antenna to take over smartphones with headphones plugged in via the Google Now and Siri personal assistants. The attack utilizes the device's headphone cord as an antenna, and can enable hackers to force phones to send emails and messages, visit malicious sites, or become an eavesdropping device. http://www.net-security.org/secworld.php?id=18984

(International) Officials: Hacker who ID'd U.S. military members for ISIS arrested. The U.S. Department of Justice reported October 16 that a Kosovo citizen will be extradited to the U.S. from Malaysia for allegedly hacking into the computer systems of a U.S.-based company and stealing the personal information of 1,351 U.S. military and other government personnel in order to share it with ISIS militants between June and August 2015. The suspect is believed to be the leader of the Kosova Hacker's Security Internet hacking group.

http://abc13.com/news/officials-hacker-who-idd-us-military-members-for-isis-arrested/1035894/

Banking and Finance Industry

(National) Dow Jones suffers data breach. Dow Jones & Company alerted customers October 9 after discovering that hackers targeted contact details of current and former subscribers between August 2012 – July 2015, and may have accessed financial information belonging to 3,500 individuals. There is reportedly no direct evidence that any information was stolen or misused, and law enforcement officials believe that the attack was linked to a broader hacking campaign. http://www.securityweek.com/dow-jones-suffers-data-breach

(National) E-Trade notifies 31,000 customers that their contact info may have been breached in 2013 hack. E-Trade notified about 31,000 customers in the week of October 5 that their personal information including email account names and physical names and addresses may have been compromised in a 2013 cyberattack. The company reportedly warned customers out of an abundance of caution and found no fraud or losses resulting from the incident. https://www.washingtonpost.com/news/the-switch/wp/2015/10/09/e-trade-notifies-31000-customers-that-their-contact-info-may-have-been-breached-in-2013-hack/

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(National) Dallas Zoo gift shop among several affected by security breach. Service Systems Associates, Inc., reported October 14 that its credit card payment system, used in gift shops in several zoos including the Dallas Zoo, Houston Zoo, and Detroit Zoo was compromised from March 24 – May 20 after malware

breached its systems. The malware was removed and the company advised customers to contact their bank for any fraudulent activity. http://thescoopblog.dallasnews.com/2015/10/dallas-zoo-gift-shop-among-several-affected-by-security-breach.html/

(National) Uber accidentally leaks personal information of hundreds of U.S drivers. Uber Technologies Inc., reported October 16 that the personal information of 674 drivers, included driver's license scans, Social Security numbers, and tax forms, among other confidential data was accidentally leaked October 13 from the new Uber Partner app designed to provide service information to the company about its drivers. Uber resolved the issue and alerted drivers of the breach through online forums such as Reddit. http://www.techtimes.com/articles/95617/20151016/uber-accidentally-leaks-personal-information-of-hundreds-of-us-drivers.htm

(National) Payment card breach at Peppermill Resort Spa Casino in Reno. Officials reported October 16 that a breach at the front desk of the Reno, Nevada-based Peppermill Resort Spa Casino may have compromised an undisclosed number of individuals' personal information, including card numbers, expiration dates, and credit card security codes from October 2014 -- February 2015. Peppermill Resort Spa Casino implemented new policies and procedures to mitigate future incidences. http://www.scmagazine.com/payment-card-breach-at-peppermill-resort-spa-casino-in-reno/article/447433/

Communications Sector

Nothing Significant to Report

Critical Manufacturing

Nothing Significant to Report

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

Nothing Significant to Report

Energy

Nothing Significant to Report

Food and Agriculture

Nothing Significant to Report

Government Sector (including Schools and Universities)

(National) **Computer glitch temporarily knocks out U.S. Customs processing system.** The U.S. Customs and Border Protection announced that it experienced a 90-minute outage October 14 with its processing systems at airports of entry in the U.S. International travelers were processed with substitute procedures while the technical disruption was addressed.
http://miami.cbslocal.com/2015/10/14/computer-glitch-temporarily-knocks-out-u-s-customs-processing-system/

Information Technology and Telecommunications

(International) Attackers compromise Cisco Web VPNs to steal login credentials, backdoor target networks. Security researchers from Volexity discovered that attackers are continuing to leverage unpatched vulnerabilities or finding ways to gain administrator access to networks via Cisco Clientless secure sockets layer (SSL) virtual private network (VPN) portals in order to harvest employee credentials by injecting malicious JavaScript code on login pages to the VPN. The attackers are reportedly targeting academic institutions, medical facilities, electronics and manufacturing businesses, and government organizations.
http://www.net-security.org/secworld.php?id=18958

(International) WordPress XML-RPC service used to amplify brute-force attacks. Security researchers from Sucuri discovered a variation of brute-force attacks that is utilizing WordPress' built-in extensible markup language remote procedure call (XML-RPC) feature to amplify attacks by bundling together hundreds and thousands of administrative username and password combinations. Researchers recommend deleting the plugin if it is not being used.
http://news.softpedia.com/news/wordpress-xml-rpc-service-used-to-amplify-brute-force-attacks-494170.shtml

(International) Cisco IOS rootkits can be created with limited resources: Researchers. Security researchers from Grid32 released research revealing that cybercriminals could easily create a basic Cisco IOS rootkit within a month or less which could rival the effectiveness of the SYNful Knock malware designed to replace router firmware. Cisco has implemented several new security technologies in current devices to help mitigate threats.
http://www.securityweek.com/cisco-ios-rootkits-can-be-created-limited-resources-researchers

(International) Thousands of Zhone SOHO routers can easily be hijacked. A security researcher from Vantage Point Security revealed a number of recently patched vulnerabilities, including a remote code execution (RCE) flaw in Zhone Technologies Small Office/Home Office (SOHO) routers, and reported - 6 - that some users could not access the products' administration panels to apply the corresponding firmware update.
http://www.net-security.org/secworld.php?id=18967

(International) Kaspersky Antivirus fixes bug that allowed attackers to block Windows Update and other services. Kaspersky Antivirus fixed a flaw in its Internet Security package's Network Attack Blocker component that could have allowed an attacker to spoof traffic and to use the product to block services such as Microsoft Windows Update, Kaspersky's update servers, or other services that would enable a system to be compromised further. The company reported that the flaw had never been exploited in the wild.
http://news.softpedia.com/news/vulnerability-open-to-abuse-fixed-in-kaspersky-internet-security-antivirus-494280.shtml

(International) DDoS attacks can bypass mitigation services by taking aim at a website's origin IP. Security researchers from the U.S. and Belgium released research revealing that most Cloud-Based Security Providers' (CBSP) distributed denial-of-service (DDoS) mitigation can be bypassed by attackers who discover targeted Web site's origin Internet protocol (IP) addresses either by analyzing outbound connections, Secure Sockets Layer (SSL) certificates, via sensitive files hosted on the server, or during migration or maintenance operations that expose the site. Researchers found that 71.5 percent of 17,877 scanned Web sites revealed origin IP addresses.
http://news.softpedia.com/news/ddos-attacks-can-bypass-mitigation-services-by-taking-aim-at-a-website-s-origin-ip-494273.shtml

(International) Chrome 46 patches vulnerabilities, simplifies page security icon. Google announced the release of version 46 of its Chrome Web browser, which addresses 24 security vulnerabilities including a cross-origin bypass in the Blink rendering engine, a user-after-free in PDFium and ServiceWorker, and a bad cast issue in PDFium, among others. The update also changed the icon used for Hypertext Transfer Protocol Secure (HTTPS) connections.
http://www.securityweek.com/chrome-46-patches-vulnerabilities-simplifies-page-security-icon

(International) Netgear publishes patched firmware for routers under attack. Netgear published firmware updates addressing a remotely exploitable authentication bypass vulnerability that hackers had exploited to take over up to 10,000 routers, most of which were in the U.S. The flaw allowed an attacker to access the device's administration interface without knowing the router

password. https://threatpost.com/netgear-publishes-patched-firmware-for-routers-under-attack/115006/

(International) Nuclear EK generates Flash exploits on-the-fly to evade detection. Security researchers from Morphisec discovered that the Nuclear exploit kit (EK) is generating different variations of an Adobe Flash exploit on-the-fly throughout the day and changing host Web sites that victims are being directed to hourly in an effort to bypass detection. The EK also tracks victims' Internet protocol (IP) addresses to prevent the same exploit combination being served to the same victim twice.
http://www.securityweek.com/nuclear-ek-generates-flash-exploits-fly-evade-detection

US-CERT Updates and Vulnerabilities

Adobe Releases Security Updates for Flash Player. Adobe has released security updates to address multiple vulnerabilities in Flash Player. Exploitation of some of these vulnerabilities may allow a remote attacker to take control of an affected system. Users and administrators are encouraged to review Adobe Security Bulletin APSB15-27(link is external) and apply the necessary updates.
https://helpx.adobe.com/security/products/flash-player/apsb15-27.html

Apple Releases Security Updates for Keynote, Pages, and Numbers. Apple has released security updates for Keynote, Pages, and Numbers for OS and iOS to address multiple vulnerabilities. Exploitation of some of these vulnerabilities may allow a remote attacker to take control of an affected system.
https://support.apple.com/en-us/HT205373

Mozilla Releases Security Update for Firefox. Mozilla has released Firefox 41.0.2 to address a security vulnerability. Exploitation of this vulnerability may allow a remote attacker to obtain sensitive information from an affected system. US-CERT encourages users and administrators to review Mozilla Security Advisory

2015-115 and apply the necessary update. https://www.mozilla.org/en-US/security/advisories/mfsa2015-115/

Google Releases Security Update for Chrome. Google has released Chrome version 46.0.2490.71 to address multiple vulnerabilities for Windows, Mac, and Linux. Exploitation of some of these vulnerabilities may allow a remote attacker to take control of an affected system. Users and administrators are encouraged to review the Chrome Releases(link is external) page and apply the necessary update. http://googlechromereleases.blogspot.com/2015/10/stable-channel-update.html

Microsoft Releases October 2015 Security Bulletin. Microsoft has released six updates to address vulnerabilities in Microsoft Windows. Exploitation of some of these vulnerabilities could allow an attacker to take control of an affected system. https://technet.microsoft.com/en-us/library/security/ms15-oct.aspx

Adobe Releases Security Updates for Reader, Acrobat, and Flash Player. Adobe has released security updates to address multiple vulnerabilities in Reader, Acrobat, and Flash Player. Exploitation of some of these vulnerabilities may allow a remote attacker to take control of an affected system. Users and administrators are encouraged to review Adobe Security Bulletins APSB15-24 (https://helpx.adobe.com/security/products/reader/apsb15-24.html) and APSB15-25 (https://helpx.adobe.com/security/products/flash-player/apsb15-25.html) and apply the necessary updates.

ICS-CERT Alerts & Advisories

ICS-ALERT-15-288-01 : **SDG Technologies Plug and Play SCADA XSS Vulnerability**
NCCIC/ICS-CERT is aware of a public disclosure of a cross-site scripting vulnerability with proof-of-concept (PoC) exploit code affecting SDG Technologies Plug and Play SCADA, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. According to this report, the vulnerability is exploitable by inserting malicious script in the HTML request to web servers.

ICSA-15-288-01 : **3S CODESYS Runtime Toolkit Null Pointer Dereference Vulnerability** This advisory provides mitigation details for a NULL pointer dereference vulnerability in the 3S-Smart Software Solutions GmbHs CODESYS Runtime Toolkit.

ICSA-15-286-01 : **Nordex NC2 XSS Vulnerability**
This advisory provides mitigation details for a cross-site scripting vulnerability in the Nordex NC2 Wind Farm Portal application.

Public Health

(Maryland) Audit: Maryland health-insurance site failed to protect patient information. The Maryland Office of Legislative Audits released a report October 9 which found that the operators of Maryland Health Benefit Exchange's Web site improperly stored Social Security numbers and other customer information, while awarding over $100 million in contracts without ensuring that the money was being properly spent. The exchange stated that it took steps to increase security measures and safeguards to help protect consumer information.
https://www.washingtonpost.com/local/dc-politics/audit-maryland-health-insurance-site-failed-to-protect-patient-information/2015/10/09/68f70a14-6e9f-11e5-9bfe-e59f5e244f92_story.html

Transportation

(National) Outdated technology likely culprit in Southwest Airlines outage. Southwest Airlines issued a statement October 12 that technical systems were repaired after a computer glitch prevented passengers from checking in and caused 836 delays out of 3,355 flights scheduled October 11. The cause of the failure is believed to be from outdated technology.
http://www.nbcnews.com/business/travel/outdated-technology-likely-culprit-southwest-airlines-outage-n443176

Water and Dams

Nothing Significant to Report

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165